HealthManagement
Promoting Management and Leadership

U.S., Canada issue joint alert on 'ransomware' after hospital attacks

The United States and Canada warned against ransomware following a wave of incidents in both countries where healthcare facilities have been forced to pay hackers to unlock encrypted data.

The warning was issued in a rare joint cyber alert as several security firms said they expected the number of incidents to rise as hackers become more savvy and few organisations invest in proper IT security.

"Infections can be devastating to an individual or organisation, and recovery can be a difficult process that may require the services of a reputable data recovery specialist," the two governments said in the alert, distributed by the U.S. Department of Homeland Security and the Canadian Cyber Incident Response Centre.

In addition to hospitals, businesses, government agencies, individual and police departments have fallen victim to cybercriminals over the past few months.

Thursday's alert detailed the impacts of ransomware attacks saying they trigger a loss of sensitive or proprietary information, disruption of regular operations, expenses to restore access to computer systems and harm to a victim's reputation. It also discourages paying cybercriminals ransom to regain access to data.

"Paying the ransom does not guarantee the encrypted files will be released. It only guarantees that the malicious actors receive the victim’s money, and in some cases, their banking information."

Since the start of this year, there have been several publicised incidents of healthcare hacking.

MedStar in Washington shut down much of its computer network last week to halt the spread of a virus and there were reports that hackers had demanded a ransom of $18,500 for restoration of a normal service.

Last month, Hollywood Presbyterian Hospital in Los Angeles paid a ransom of $17,000 to hackers to re-access blocked data.

Meanwhile, experts have warned about a new virus threatening cybersecurity. PowerWare is delivered vie email and appears to be an invoiice, much like Locky. Once the invoice is opened, the computer system is locked down until a ransom is paid. It also mimics legitimate computer files and activiites.

Source: Reuters

Image Credit:CRWFlags

Published on : Mon, 4 Apr 2016